Security
Data Sheet

IBM Trusteer Rapport

Provide banking with malware detection and remediation, phishing detection and protection

Highlights

- Use machine learning and advanced analytics to help detect and protect against phishing attacks
- Help detect and protect against financial malware infections and reduce false positives
- Remove existing financial malware
- Protect browser sessions against tampering and key-logging attacks
- Continuously adapt to emerging threats throughout the fraud lifecycle

As financial institutions seek to make a digital transformation to capture new opportunities through channels such as online banking, it becomes increasingly critical to both provide a seamless user experience and help protect against online fraud. But fraudsters continue to successfully modify their attack methods to keep pace with this transformation, stealing credentials with sophisticated email content and other tactics and using technology to bypass common phishing detection logic.

Meanwhile, customers increasingly use online banking. After all, immediate, 24x7 access to account information is a tremendous benefit for them—and, unfortunately, a tremendous advantage for cybercriminals.

To meet these challenges, hundreds of financial institutions and tens of millions of their customers rely on IBM® Trusteer® Rapport® to help protect their desktops against fraud.

Designed specifically for the financial industry, Trusteer Rapport provides capabilities backed by a global footprint and industry-leading security researchers, technology and processes—that enable organizations to achieve sustainable fraud detection and regulatory readiness.

Can your financial institution automatically detect and prevent phishing attacks? Doing so would certainly benefit your customers, especially when phishing websites continuously pop up targeting online banking. But swiftly identifying and taking down these websites is time-consuming—and unfortunately, most users submit their credentials in the first few hours of the attack. As a result, to guard against phishing you need to the ability to protect end users as soon as the phishing campaign launches—and at the moment they are most vulnerable, when they're about to disclose their credentials or payment card data.

Getting ahead of the fraud and malware threat

Trusteer Rapport is designed to help organizations protect their critical resources with:

- **Automated phishing detection capabilities:** Trusteer Rapport uses machine learning to analyze unstructured website data—including links, images, forms, text, scripts, Document Object Model (DOM) data, URLs and more. It then leverages robust analytics and global security intelligence data to help financial institutions protect their customers from phishing attacks at a speed and scale like never before.
- **Malware protection based on actionable insight:** Using intelligence gathered from millions of protected endpoints, Trusteer processes tens of thousands of malware attack attempts every day, creating a compact and actionable footprint of cybercrime targets and tactics. The process enables financial institutions to rapidly adapt to emerging threats—including zero-day attacks—by automatically integrating countermeasures to help promptly detect and block attacks on protected endpoints.
- **Global threat intelligence:** Trusteer technology transparently secures the browser and sensitive client applications against malware and phishing attacks to help detect and protect against malware tampering with these applications, while immediately alerting Trusteer Rapport to any abnormal behavior that could represent a new attack.

Phishing protection that's more timely than ever

In the fight against phishing, speed to detection is critical. The majority of successful attacks occur within the first hour of a fraudulent website's appearance online.

Trusteer Rapport helps detect and protect against credential and personal information theft with a new and different cognitive approach designed to protect customers from phishing attacks when they navigate to fraudsters' bogus websites. If an end user navigates to a phishing website, Trusteer Rapport uses a layer of phishing detection with patented machine learning algorithms and advanced analytics to rapidly identify the activity and provide immediate and automatic analysis of the website. And Trusteer Rapport does it at a speed that would be impossible for a human analyst to achieve.

If Trusteer Rapport confirms that the website is a phishing website, the solution can notify or block the end user immediately to help prevent the theft of credentials and payment card data, stopping the subsequent fraud that otherwise would follow.

This new cognitive approach to phishing detection is in stark contrast to conventional anti-phishing takedown services that can require several hours to respond to an attack[1]—an ample period in which many customers can be compromised.

Malware prevention and removal of existing malware

Once installed, Trusteer Rapport removes existing financial malware from end-user devices and helps detect and protect against future infections by stopping attempts to exploit browser vulnerabilities and install malware on the endpoint. Trusteer Rapport provides a simple way for fraud and support teams to remediate threats on endpoints and resume safe online banking.

Protect transactions with holistic fraud detection

Trusteer Rapport provides multi-layered protection across customer devices and the transaction lifecycle.

To help defend against man-in-the-browser and man-in-the-middle attacks, the solution can lock down the browser to help protect against malicious web page injection attacks designed to social engineer victims into surrendering personal information or approving fraudulent transactions.

Trusteer Rapport blocks man-in-the-middle attacks by validating online banking IP addresses and Secure Sockets Layer (SSL) certificates belonging to the genuine site.

Trusteer Rapport further helps protect against the theft of login credentials and personal information by disabling key-logging and screen-capturing attempts of sensitive application pages, such as login and money transfer pages.

Financial institutions receive Trusteer intelligence alerts on malware and phishing activity identified by Trusteer Rapport. The alerts can further drive fraud-prevention and mitigation processes such as user recredentialing, transaction reviews and more.

Count on client deployments and support

Trusteer Rapport is offered to end users during login through an out-of-the-box “splash” message, enabling easy opt-in or mandatory deployment. The process enables the financial institution to customize when it offers Trusteer Rapport to its customers—for example, to protect high-risk transactions or customers who have previously experienced fraud. Deployment respects the customer’s privacy, doesn’t burden devices and won’t conflict with anti-virus products—so users can readily go about their online activity, knowing they are protected.

Trusteer Rapport clients are deployed and maintained by IBM, with automatic updates, to help continuously protect customers against new threats. IBM offers dedicated 24x7 end-user support to address any technical questions end users may have during installation or when using the product.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for fraud detection and identity and access management. These technologies enable organizations to protect their customers, employees and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and Business Partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

For more information

To learn more about IBM Trusteer Rapport, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] “Global Phishing Survey: Domain Name Use and Trends in 2H2014,” *Anti-Phishing Working Group (APWG)*, May 27, 2015. http://www.antiphishing.org/download/document/245/APWG_Global_Phishing_Report_2H_2014.pdf

Please Recycle